Privacy Policy for the
University of Toronto Mississauga

Access to Information

At the University, information, which is not public, is classified and treated as confidential. Staff at UTM have access to a range of confidential information. One key type of confidential information is personal information, which is information about an identifiable individual, which may include, but is not limited to, faculty, staff and students. A University employee is only permitted to access personal information as necessary to fulfill job responsibilities, and information must be treated in a manner consistent with the purposes for which it was collected. Personal information must not be released to or discussed with anyone other than the individual whose information is involved, or other University staff who also need the personal information to do their jobs, or unless the individual has given explicit consent. Responsibility for following this “need-to-know” principle rests with everyone at the University. Both a University official seeking the personal information and an official who may disclose it are responsible for ensuring that the disclosure is properly executed.

It is a legal responsibility of the university to ensure that personal information is kept confidential and secure, and only accessed on a need-to-know basis.

The following guidelines set out required practices to ensure that UTM faculty and staff meet this obligation. If you have any questions or special requirements, please discuss these with your supervisor or contact the UTM FIPPA Liaison, in the Office of the Campus Council, 905-828-5233; cindy.ferencz@utoronto.ca.

More detailed information is available in the guidelines developed by the Office of the Vice-President and Provost titled Access and Privacy Practices: General and Administrative:

http://uoft.me/AccessandPrivacyPractices

Electronic information

- Storing confidential information on a USB key or your computer’s hard drive:

Confidential information, including personal information (such as names, student numbers, contact information, academic information, financial information, etc.)
should not be stored on local devices (e.g. your computer’s hard drive or a USB key). This information should be held in a secure server environment with appropriate restricted user rights. If there is an exceptional circumstance requiring local storage, the storage device must be encrypted to ensure all files stored on the device are always encrypted.

- Transporting personal information outside the office:

Personal information should not be transported outside the office, whether on a laptop or portable storage device such as a USB key, or kept on a home computer. Because of the sensitivity of this information, this is the case even when the information is encrypted. A Director must approve any exceptions in advance, and the approval must be documented before the information is stored or transported outside the office.

- Security of Computers

All computers require both physical and system protection, which provide a security baseline for computers that are to house and access confidential records or data.

The following are required practices that help to ensure that computer, software and data are appropriately and effectively protected:

- Prompt software and security updates, including operating systems and anti-virus programs;
- Full disk encryption;
- Sound user account practices, including strong passwords;
- Physical security of the machine;
- Suitable data backups.

- Security of Mobile Devices

Any mobile device or data store (phone, laptop, tablet, USB key etc.) that is to be used to hold or transport personal and/or other confidential information must do so with either the data fully de-identified, the data encrypted, or full device encryption. Access passwords or pins for devices must also be of suitable length and complexity and should be changed regularly.

- Transmission of data / Email Security

With the exception of internal email (from one UTOR address to another UTOR address), email is not a secure form of communication. Use of email to share personal information should be limited to cases when there are no reasonable alternatives and attachments with confidential information should be password
protected. Passwords for encrypted attachments should be communicated by another means, such as telephone, rather than by email.

If it is necessary to access confidential information from campus, access should only be via institutionally approved virtual private network (VPN) or secure remote desktop connection.

- Equipment retirement/disposal

When the time comes to retire equipment, any data stored on it must be reliably destroyed prior to it leaving the custody of the university. Computers, phones, scanners, printers, flash drives, laptops and other equipment can all retain data or metadata that is considered confidential. Typical decommissioning will involve at least three full rewrites of storage media/devices with random data as a minimum standard. If a third party is to decommission the equipment, as is often the case with printers and multifunction devices for example, written confirmation from that party is required that the data have been securely and confidentially destroyed to industry standards.

For computer and data security assessments and consultation regarding full-disk-encryption, mobile device security options, network storage and secure remote access options please contact the UTM IITS Help Desk at helpdesk.utm@utoronto.ca or phone 905-828-5344.

Paper documents

As with electronic information, paper documents and files containing personal information are highly confidential. These should be placed in locked cabinets overnight or during absences from the office, and office doors should be locked. This follows the principle of protecting documents behind two levels of locks – one on the building and/or office, and another on a secure cabinet.

Electronic document storage and management on secure University servers is encouraged as a means to reduce the risks and storage load of hard copy records.

Particular care should be exercised when transporting hard copy records outside the office. This should only be done when absolutely necessary and with the knowledge and permission of your Director. If you must take files home, take as few at a time as possible, take copies rather than originals, and ensure they are always with you during transit. Do not leave them unattended, for example, in a parked car. Any confidential and/or personal information that is taken home must be locked when not in use.
The UTM Office of the Registrar has developed a standard operating procedure for dealing with student information received in paper form. Such information is transferred to a secure electronic format as soon as possible. More detail is available from that office.

Always use a cross-cut shredder to destroy confidential paper records.

**Clean desk policy**

When leaving your office, ensure that all confidential documents, including documents with personal information, are locked in a cabinet or drawer.

**Parents and third parties**

The university often receives requests from parents or other third parties for access to student information; these individuals may be persistent in their inquiries. Parents do not have a right to such information; in fact, privacy legislation explicitly prevents the university from sharing any personal information with a third party unless the individual (e.g., the student) has consented. Only share student information with a parent if there is previous written authorization from the student, or the student attends in person and authorizes the sharing.

**Emergency situations**

We have an obligation to provide personal information in compelling circumstances that affect the health or safety of an individual, where providing that information would help to reduce the health or safety concern. Health and safety trump privacy. Consult your manager or director whenever there is a health or safety concern, and be sure that you follow the University’s Emergency Disclosure of Personal Information guideline:

http://uoft.me/emergencysituations

**Loss of information**

If any personal information is lost or misplaced, e.g., a document, file, USB key, laptop, etc., you have an obligation to report this immediately to the UTM FIPPA Liaison, in the Office of the Campus Council, 905-828-5233; cindy.ferencz@utoronto.ca. In such cases, please notify your Director immediately. Consequences can best be controlled with quick intervention.

**Additional security measures**

Cameras have been installed throughout UTM.